REMARKS

This preliminary amendment is to amend portions of the specification and claims to restore information that may have been omitted due to a clerical error that caused the omission of a single line of the non-English language text on multiple pages of the specification and claims as filed. The proposed amendments however are supported based on related other portions of the specification and claims as filed and accordingly do not constitute new matter.

Upon review of the filed application copy in our records, it became apparent that the copy of the original document may have inadvertently omitted a first line on a number of pages. Additionally, Figure 8 was apparently inadvertently not copied. Figure 8 did not contribute to any claimed subject matter. Hence, the drawing description of Figure 8 and the only reference to Figure 8 in the specification are removed.

A careful review of the actual technical information filed in the specification and claims along with Figures 1-7 was undertaken and confirmed that the claims are more than adequately supported and disclosed in the actual application as filed in the U.S. Patent Office on July 18, 2003.

Accordingly, Applicant wishes to keep the filing date for the actual specification and drawings and seeks to provide an amended specification and claims that are fully supported to address the omitted lines of text with this Preliminary Amendment.

As a courtesy to the Examiner, copies of five source documents (Source #1 to Source #5) are included with this amendment. These five source documents show an unbroken chain of correspondence from the original Japanese language specification and claims (Source #1) as filed to the newly submitted English language translation of the specification (Source #5) as filed.

Source #1 is a file copy of the original Japanese language specification and claims as filed in the present application. Applicant respectfully submits that Source #1 may be missing an initial first line of text on 17 pages due to a clerical error in reproducing the original document. Each missing line is hereinafter referred to as a numbered omission (Omission #1 to Omission #17) and amendments to the English language translation are submitted to replace the omitted text based on the support provided by other portions of the application as filed.

Source #2 is a complete Japanese language version of Source #1 with a circled number identifying each of the 17 omissions. The initials "GG" in proximity to Omissions #2-#17 are provided by a translator as described below. Omission #1 is an English language portion and was not addressed by the translator. Source #2 includes the original Japanese language drawing Figures 1-7.

Source #3 is a certified English language translation of Source #2 and includes the specification, claims, and drawings without regard to the omitted text of Source #1. The translation of Source #3 originally included Figure 8 that was omitted as discussed above.

Source #4 is the certified English language translation of Source #2 with an additional certification that the underlined and numbered text corresponds to the similarly numbered and circled text omissions identified in Source #2. The identified portions the Source #2 that bear a circled number (2) through (17) and a translator's hand-written initials "GG" correspond to the similarly numbered and underlined portions of Source #4 that bear the hand-written initials as described in the certification statement at the end of Source #4.

Source #5 is a copy of Source #4 with underlined blanks corresponding to the portions of the text omitted from the specification as filed. Applicant respectfully submits Source #5 is believed to be an accurate translation of the original Japanese language specification as filed

where the underlined blanks indicate the location of the omitted text as described in reference to Source #1 through Source #4. Specifically, Source #5 relies on the certified translation of Source #3 and the certified locations of the missing text identified in Source #4 to produce what is believed to be an accurate translation of the application as filed. All references to the specification hereinafter are referenced to the translation shown in Source #5. The following is a discussion of how the omitted text is supported by other portions of the application as filed.

Regarding Omission #1, the paragraph on page 2 ll. 19-20 is amended to indicate the reference "Document 2:" which is impliedly understood from the position of the omitted text in the document listing between Document 1 and Document 3 (Specification page 2 ll. 16 and 21). Omission #1 was not addressed by the translator in Source #4 since the omitted portion is already in the English language. The entire citation of the original reference for Document 2 is supplied in the Information Disclosure Statement supplied herewith.

Omission #2 shown as the circled (2) on page 3/21 line 1 of Source #2 corresponds to the underlined portion (2) on page 3 line 26 to page 4 line 2 of Source #4. The paragraph from page 3 line 20 to page 4 line 2 is amended to include the omitted information that is repeated in Claim 1 on page 28 ll. 7-9.

Omission #3 shown as the circled (3) on page 4/21 line 1 of Source #2 corresponds to the underlined portions (3a-3c) on page 6 lines 1 to 8 of Source #4. The paragraph from page 5 line 23 to page 6 line 9 is amended to include "is more effective in" reducing the amount of calculation than the approach to find keys for respective rounds separately (Specification page 27 ll. 1-9). The paragraph is amended to include the transitional language "Further" which is impliedly supported by the sentence structure. Finally, the paragraph is amended to include the calculations of all session key prospects for each round are completed before calculating the

session key prospects for the immediately preceding round (Specification page 18 ll. 19-20 and page 24 ll. 1-9).

Omission #4 shown as the circled (4) on page 5/21 line 1 of Source #2 corresponds to the underlined portions (4a-4d) on page 8 lines 3 to 10 of Source #4. The paragraph from page 7 line 23 to page 8 line 14 is amended to include the omitted information that is repeated in Claim 2 on page 31 line 22 to page 32 line 4.

Omission #5 shown as the circled (5) on page 6/21 line 1 of Source #2 corresponds to the underlined portion (5) on page 10 lines 9 to 10 of Source #4. The paragraph on page 10 lines 4-11 is amended to include the omitted information that is repeated in Claim 3 on page 33 ll. 21-22.

Omission #6 shown as the circled (6) on page 7/21 line 1 of Source #2 corresponds to the underlined portions (6a-6b) on page 12 lines 12 to 14 of Source #4. The paragraph on page 12 lines 11-16 is amended to include the information that is repeated in Claim 4 on page 35 ll. 13-15.

Omission #7 shown as the circled (7) on page 8/21 line 1 of Source #2 corresponds to the underlined portion (7) on page 14 lines 20 to 23 of Source #4. The paragraph on page 14 lines 13-23 is amended to include the brute-force search in the immediately succeeding round using the transforming block (Specification page 12 ll. 17-21 and page 18 ll. 7-9). The brute-force search is employed for the immediately succeeding round (Specification page 27 ll. 1-4).

Omission #8 shown as the circled (8) on page 9/21 line 1 of Source #2 corresponds to the underlined portion (8) on page 16 lines 1 to 2 of Source #4. The paragraph from page 15 line 24 to page 16 line 6 is amended to include transitional language "and includes" that is impliedly understood from sentence structure that follows along with the construction shown in Fig. 2.

Omission #9 shown as the circled (9) on page 10/21 line 1 of Source #2 corresponds to the underlined portion (9) on page 17 line 20 of Source #4. The paragraph on page 17 lines 16-21 is amended to complete the verb construction "is configured" as supported by the sentence structure.

Omission #10 shown as the circled (10) on page 11/21 line 1 of Source #2 corresponds to the underlined portions (10a-10b) on page 19 lines 18 to 19 of Source #4. The paragraph on page 19 lines 16-19 is amended to include the cryptanalysis employing a 7th order differential is described in the preceding text and by the following equation for the sub-space (Specification page 19 ll. 9-10 and 20-23). Further, the notation $V^{(7)}$ is well known in the relevant art to refer to a sub-space in this context.

Omission #11 shown as the circled (11) on page 13/21 line 1 of Source #2 corresponds to the underlined portions (11a-11b) on page 22 lines 11 to 15 of Source #4. The paragraph on page 22 lines 8-23 is amended to include the information that is repeated on page 24 ll. 4-8.

Omission #12 shown as the circled (12) on page 14/21 line 1 of Source #2 corresponds to the underlined portions (12a-12c) on page 24 lines 13 to 18 of Source #4. The paragraph on page 24 lines 9-18 is amended to include "creates conditions" as supported in the phrase "conditions thus created" within the same sentence (Specification page 24 line 17) as well as creating the conditions based on an algebraic method (Specification page 14 ll. 13-16). The paragraph is amended to include outputting an uncalculability identifier if the conditions are inconsistent with each other (Specification page 21 ll. 23-25).

Omission #13 shown as the circled (13) on page 15/21 line 1 of Source #2 corresponds to the underlined portion (13) on page 26 lines 21 to 23 of Source #4. The paragraph on page 26 lines 13-23 is amended to include the application of the estimation of a cipher from a different

cipher strength estimating device since the complex of different transformation rounds does not appear to be adequately supported in the specification as filed.

Omission #14 shown as the circled (14) on page 17/21 line 1 of Source #2 corresponds to the underlined portions (14a-14b) on Claim 1 on page 28 line 2 and page 30 lines 1 to 2 of Source #4. Claim 1 is amended to include the omitted information as found in Claim 1 line 7 regarding "the cipher strength estimating device comprising" and page 5 ll. 20-21 that repeats the omitted text.

Omission #15 shown as the circled (15) on page 18/21 line 1 of Source #2 corresponds to the underlined portions (15a-15b) of Claim 2 on page 30 line 5 and page 32 lines 6 to 7 of Source #4. Claim 2 is amended to include the omitted information as found in Claim 2 line 6 regarding "the cipher strength estimating device comprising" and page 8 line 13 that repeats the omitted text.

Omission #16 shown as the circled (16) on page 19/21 line 1 of Source #2 corresponds to the underlined portions (16a-16c) of Claim 3 on page 34 lines 11 to 14 of Source #4. Claim 3 is amended to include the omitted information as found in Claim 3 line 7 regarding "the cipher strength estimating device comprising" and page 10 line 26 to page 11 line 3 that repeats the omitted text.

Omission #17 shown as the circled (17) on page 20/21 line 1 of Source #2 corresponds to the underlined portions (17a-17b) of Claim 4 on page 36 lines 11 to 14 of Source #4. Claim 4 is amended to include the omitted information as found in Claim 4 line 7 regarding "the cipher strength estimating device comprising" and page 13 ll. 10-13 that repeats the omitted text.

Regarding Figure 8, the paragraph on page 15 ll. 18-19 from the Brief Description of the Drawings is deleted and the paragraph on page 21 ll. 5-7 is amended to remove any reference to

the figure itself while including the description of the figure. Figure 8 was apparently inadvertently not copied prior to filing the present application. Figure 8 was directed to alternative structures and illustrated the algebraic comprehension of key movement or transformations in relation to one of the discussed conditions but did not contribute to any claimed subject matter.

If the Examiner believes that a telephone interview will help further the prosecution of this case, the Examiner is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

On: 1-26-04
Date

By: James Lee
Printed Name

Signature

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920